CyberArk

Privileged Access Manager – Digital Vault Server v14.0

Security Target

Version 1.8

Jun 2024

Document prepared by

Lightship Security

www.lightshipsec.com

Document History

Version	Date	Author	Description
0.1	08 Sept 2021	Marina Ibrishimova	First draft.
0.2	09 Nov 2021	Marina Ibrishimova	Updated ST to APP PP v1.4
0.3	19 Sep 2022	Marina Ibrishimova	Added latest TDs.
0.4	09 Oct 2022	Marina Ibrishimova	Addressed vendor’s comments.
0.5	01 Jan 2023	Marina Ibrishimova	Addressed evaluator’s comments.
0.6	21 Feb 2023	Marina Ibrishimova	Addressed evaluator’s comments.
0.7	16 Apr 2023	Marina Ibrishimova	Addressed evaluator’s comments.
0.8	25 Apr 2023	Marina Ibrishimova	Addressed ALC observations.
0.9	11 Oct 2023	Marina Ibrishimova	Added latest TDs.
1.0	16 Oct 2023	Marina Ibrishimova	Addressed vendor comments.
1.1	17 Dec 2023	Marina Ibrishimova	Addressed ASE comments.
1.2	24 Jan 2024	Enav Coresh	Addressed ASE comments.
1.3	30 Jan 2024	Enav Coresh	Addressed ASE comments.
1.4	11 Feb 2024	Enav Coresh	Updated product name
1.5	8 Apr 2024	Marina Ibrishimova	Addressed ASE comments.
1.6	9 May 2024	Marina Ibrishimova	Addressed ASE comments.
1.7	16 May 2024	Marina Ibrishimova	Addressed ASE comments.
1.8	13 Jun 2024	Marina Ibrishimova	Addressed ASE comments.

Table of Contents

List of Tables

1 ST Introduction

1 This Security Target (ST) defines the CyberArk Privileged Access Manager – Digital Vault Server Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The CyberArk Privileged Access Manager – Digital Vault Server is the Digital Vault Server component of the CyberArk Privileged Access Manager (PAM) solution. PAM enables organizations to secure, provision, control, and monitor all activities associated with privileged identities used in enterprise systems and applications. The TOE provides secure storage and access to privileged account files, and to the administrator and session activity files.

3 The TOE operates in a Windows environment.

1.1 ST and TOE References

Table 1: Evaluation identifiers

ST Title	CyberArk Software Ltd. Privileged Access Manager – Digital Vault Server, v14.0 Security Target
ST version	Version 1.8
ST Author	Lightship Security
ST Publication Date	Jun 13, 2024
TOE Reference	CyberArk Privileged Access Manager – Digital Vault Server v14.0.0.40

1.2 TOE Overview

1.2.1 Type

4 The TOE is an application that runs on the Windows Operating System (OS), and it is compiled with OpenSSL FIPS Object Module v1.02 and MySQL v8.0.31 database.

1.2.2 Usage

5 The TOE securely manages, stores and controls access to privileged account files, which are created by non-TOE components. The privileged account files, along with each file's unique file key, are encrypted by Privileged Access Manager (PAM) components and sent to the TOE. For each privileged account file sent to the TOE, the TOE encrypts the unique file key, and then stores the privileged account file with its TOE-encrypted file key in a logical Safe. Each Safe has a unique key, which is used to encrypt the file key of the privileged account file stored within the Safe. The encrypted privileged account files, which are sent to and retrieved by the TOE, are never decrypted by the TOE.

6 In the evaluated configuration, the TOE runs on a hardened Windows server. The TOE's network includes two additional servers for the other PAM components, LDAP server and a Certificate Authority (CA) server.

NOTE: The use of LDAP is optional. It is intended to be installed in the same physical network with the TOE, as part of the same environment. The TOE does not enforce any algorithms listed in the ST for the LDAP connection and is not responsible for the validation of the TLS parameters with LDAP.

7 Communication between the TOE and non-TOE PAM components happens over TLS as shown in Figure 1.

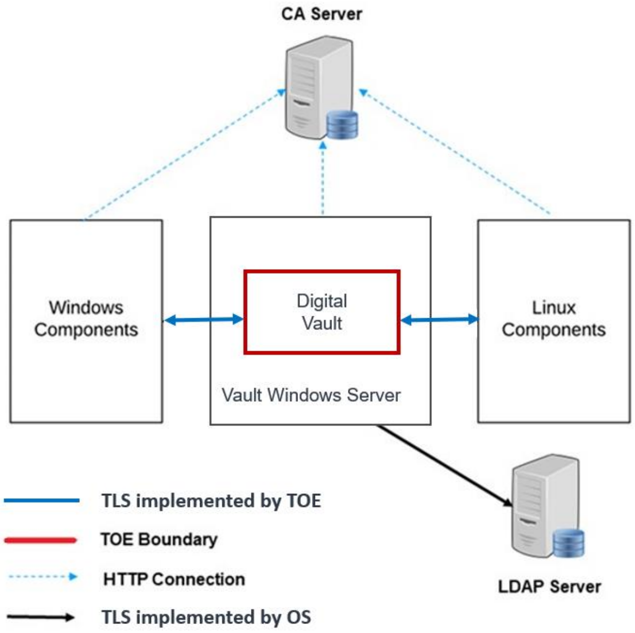

Figure 1: Example TOE deployment

1.2.3 Security Functions

8 The TOE provides the following security functions:

a) **Cryptographic Support.** The TOE implements the OpenSSL FIPS Object Module with the CyberArk libraries to provide the following cryptographic services: encryption and decryption, hashing, digital signature generation and verification, and key generation.

b) **User Data Protection.** The TOE encrypts all sensitive data stored in non-volatile memory. The TOE limits its access to network connectivity when accessing the platform’s hardware resources.

c) **Identification and Authentication**. The TOE uses X.509v3 certificates for TLS communications. The certificates are presented by the by the TOE during the TLS handshake is established. The vault certificates are authenticated by the connecting client, i.e. the Windows server PAM components, and the Linux server PAM components. The certificates can include (per generation) a CRL distribution point (CDP) to enable the clients to use a certificate revocation list (CRL) mechanisms to verify the certificate.

d) **Security Management.** The TOE provides a set of commands for administrators to manage the security functions, configuration, and other features of the TOE and OE components. A TOE administrator manages the TOE from the Password Vault Web Access (PVWA) on the Windows server in the OE. There is no access to TOE functionality until passwords are created for the built-in Administrator user.

e) **Privacy.** The TOE does not store or transmit any Personally Identifiable Identification (PII).

f) **Protection of the TSF.** The TOE leverages anti-exploitation capabilities provided by the OS. The TOE provides integrity for installation and software updates.

g) **Trusted Path.** The TOE provides a trusted path between itself and the Privileged Session Manager (PSM), Central Policy Manager (CPM), PVWA, Privileged Session Manager SSH (Secure Shell), and Proxy (PSMP) PAM components. All communications between the TOE and these components are encrypted and authenticated over TLS v1.2 (port 443) sessions.

1.2.4 Non-TOE Components

9 The TOE operates with the following non-TOE components in the environment, which are intended to be deployed in a physically secure environment:

a) PAM Windows components, OS Microsoft Windows Server 2019, is composed of the PAM components:

   i) The Privileged Session Manager (PSM) v14.0.0.9,

   PSM is the part of PAM that enables organizations to secure, control, and monitor privileged access to network devices over RDP connections.

   ii) Password Vault Web Access (PVWA) v14.0.0.32,

   PVWA is the web interface of PAM that provides a single console for requesting, accessing, and managing privileged passwords throughout the environment.

   iii) Central Policy Manager (CPM) v14.0.0.9,

   CPM automatically enforces enterprise policies for password management.

b) PAM Linux components which run on RHEL 8:

   i) Privileged Session Manager SSH (Secure Shell) Proxy (PSMP) v14.0.0.14

c) LDAP Server (optional), Windows Server 2019, a central authentication server for organizations, build to provide access to internal servers for each organization user.

d) CA Server, Windows Server 2019, provides the functionality of downloading CRLs over HTTP.

e) Vault Windows Server 2019, the server on which the TOE runs.

1.3 TOE Description

1.3.1 Physical Scope

10 The physical scope of the TOE is the Privileged Access Manager – Digital Vault Server Windows application. The TOE version is v14.0.0.40 and the TOE is delivered through CyberArk’s online customer portal, which uses AWS Marketplace.

The TOE delivery format is *.exe. The customer portal can be accessed after customers register to the portal https://cyberark.my.site.com/s/login.

1.3.1.1 Guidance Parts

11 The TOE includes the following guidance documents, which are delivered to customers through a download link that becomes available to them after they purchase the TOE and sign in for the CyberArk Privileged Access Manager - Self-Hosted customer portal:

a) Privileged Access Manager – Digital Vault Server Common Criteria Guide, v1.6 (PDF), May 2024

b) PAM Self-Hosted v14.0, 25-Jan-2024, No. A8474D5E4B6532ED3402D38B46F7DB15F650CA75EBD0372BB891F3ECDC7089CE, as follow:

Download the PAM Self hosted document described above >go to Cyberark Portal cyberark.my.site.com/mplace/s/#software > choose Privileged Access Manager Self-Hosted > go to Components > choose Documentation > download Production-PublicHelp-PAS - 14.0.zip and Extract > choose OnlineHelp.htm > choose Install and Harden components

a) Install: Installation > install PAM Self-Hosted

b) Upgrade: Installation > Upgrade

c) Admin: Administrator > Components

1.3.1.2 Configuration List

12 The evaluation package consists of the following:

a) Privileged Access Manager – Digital Vault Server (TOE)

b) Privileged Access Manager – Digital Vault Server Security Target, v1.8

c) Privileged Access Manager – Digital Vault Server Common Criteria Guide, v1.6

d) Privileged Access Manager – Digital Vault Server Entropy Description, v0.4

e) PAM Self-Hosted v14.0, 25-Jan-2024, No. A8474D5E4B6532ED3402D38B46F7DB15F650CA75EBD0372BB891F3ECDC7089CE.

1.3.1.3 Out-of-Scope Functionalities

13 The out-of-scope functionalities, which are disabled by default in the evaluated configuration are as follows:

a) Disaster Recovery Vault

b) Distributed Vault

c) Cluster Vault

d) PAM on Cloud

e) Backup (Replicate)

f) ENE (SMTP Monitoring)

g) HSM

h) Remote Control Client (SNMP Monitoring)

i) PAKeyGen

1.3.2 Logical Scope

14 The logical scope of the TOE comprises the security functions defined in section Security Functions.

1.4 Terminology

Table 2: Terminology

Term	Definition
CA	Certificate Authority
CC	Common Criteria
CPM	CyberArk Central Policy Manager
CRL	Certificate Revocation List
CDP	CRL distribution point
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
IIS	Internet information Services
LDAP	Lightweight Directory Access Protocol
NIAP	National Information Assurance Partnership
PP	Protection Profile
PAM	CyberArk Privileged Access Manager
PSM	CyberArk Privileged Session Manager
PSMP	CyberArk Privileged Session Manager SSH (Secure Shell) Proxy
PVWA	CyberArk Password Vault Web Access
SRP	Secure Remote Password
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

2 Conformance Claims

15 The following conformance claims are made:

1) CC version 3.1 Revision 5, April 2017
2) CC Part 2 extended, CCMB-2017-04-002, April 2017
3) CC Part 3 extended, CCMB-2017-04-003, April 2017
4) NIAP Protection Profile for Application Software, v1.4 (PP_APP), 2021-10-07
5) NIAP Functional Package for Transport Layer Security, v1.1, 2019-03-01, Conformant.
6) NIAP Technical Decisions per Table 3.

Table 3: NIAP Technical Decisions

TD Type	TD #	Name	Rationale if N/A
PP_APP	TD0628	Addition of Container Image to Package Format	
PP_APP	TD0650	Conformance claim sections updated to allow for MOD_VPNC_V2.3 and 2.4	
PP_APP	TD0664	Testing activity for FPT_TUD_EXT.2.2	
PP_APP	TD0717	Format changes for PP_APP_V1.4	
PP_APP	TD0719	ECD for PP APP V1.3 and 1.4	
PP_APP	TD0736	Number of elements for iterations of FCS_HTTPS_EXT.1	N/A. The TOE does not claim FCS_HTTPS_EXT.1/Server
PP_APP	TD0743	FTP_DIT_EXT.1.1 Selection exclusivity	
PP_APP	TD0747	Configuration Storage Option for Android	N/A. the TOE is not an Android app
PP_APP	TD0756	Update for platform-provided full disk encryption	
PP_APP	TD0780	FIA_X509_EXT.1 Test 4 Clarification	N/A. The TOE does not claim FIA_X509_EXT.1
PP_APP	TD0798	Static Memory Mapping Exceptions	
PP_APP	TD0815	Addition of Conditional TSS Activity for FPT_AEX_EXT.1.5	
PP_APP	TD0822	Correction to Windows Manifest File for FDP_DEC_EXT.1	

TD Type	TD #	Name	Rationale if N/A
PP_APP	TD0823	Update to Microsoft Windows Exploit Protection link in FPT_AEX_EXT.1.3	
PKG_TLS_1.1	DT0779	Updated Session Resumption Support in TLS package V1.1	
PKG_TLS_1.1	TD0770	TLSS.2 connection with no client cert	NA, this SFR is not claimed
PKG_TLS_1.1	TD0739	PKG_TLS_V1.1 has 2 different publication dates	
PKG_TLS_1.1	TD0726	Corrections to (D)TLSS SFRs in TLS 1.1 FP	
PKG_TLS_1.1	TD0513	CA Certificate loading	
PKG_TLS_1.1	TD0499	Testing with pinned certificates	
PKG_TLS_1.1	TD0469	Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1	
PKG_TLS_1.1	TD0442	Updated TLS Ciphersuites for TLS Package	

3 Security Problem Definition

16 The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any organizational security policies that the TOE is expected to enforce.

3.1 Threats

Table 4: Threats

Identifier	Description
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.

3.2 Assumptions

Table 5: Assumptions

Identifier	Description
A.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

3.3 Organizational Security Policies

17 There are no organizational security policies for the application.

4 Security Objectives

4.1 Objectives for the TOE

Table 6: Security Objectives

Identifier	Description
O.INTEGRITY	Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom, if ever, shipped without errors. The ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options.
O.QUALITY	To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behaviour relies upon using only documented and supported APIs.
O.MANAGEMENT	To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII.
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data.
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application.

4.2 Objectives for the Operational Environment

Table 7: Operational environment objectives

Identifier	Description
OE.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
OE.PROPER_USER	The user of the application software is not wilfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.
OE.PROPER_ADMIN	The administrator of the application software is not careless, wilfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

5 Security Requirements

5.1 Conventions

18 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text in square brackets.

b) **Refinement.** Indicated with bold text and strikethroughs in square brackets.

c) **Selection.** Indicated with underlined text in square brackets.

d) **Assignment within a selection.** Indicated with italicized and underlined text in square brackets.

e) **Iteration.** Indicated by adding a slash and a name, e.g., “FCS_COP.1/Hash”.

5.2 Extended Components Definition

19 All extended components (identified by EXT) are reproduced directly from the claimed Protection Profile and therefore no further definition is provided in this document.

5.3 Functional Requirements

Table 8: Summary of SFRs

Requirement	Title	Type
FCS_CKM.1/AK	Cryptographic Asymmetric Key Generation	Selection
FCS_CKM_EXT.1	Cryptographic Key Generation Services	Mandatory
FCS_CKM.2	Cryptographic Key Establishment	Selection
FCS_COP.1/SKC	Cryptographic Operation – Encryption/Decryption	Selection
FCS_COP.1/Hash	Cryptographic Operation – Hashing	Selection
FCS_COP.1/Sig	Cryptographic Operation – Signing	Selection
FCS_COP.1/KeyedHash	Cryptographic Operation – Keyed-Hash Message Authentication	Selection
FCS_RBG_EXT.1	Random Bit Generation Services	Mandatory
FCS_STO_EXT.1	Storage of Credentials	Mandatory
FCS_TLS_EXT.1	TLS Protocol	Mandatory
FCS_TLSS_EXT.1	TLS Server Protocol	Selection
FDP_DEC_EXT.1	Access to Platform Resources	Mandatory

Requirement	Title	Type
FDP_NET_EXT.1	Network Communications	Mandatory
FDP_DAR_EXT.1	Encryption Of Sensitive Application Data	Mandatory
FMT_MEC_EXT.1	Supported Configuration Mechanism	Mandatory
FMT_CFG_EXT.1	Secure by Default Configuration	Mandatory
FMT_SMF.1	Specification of Management Functions	Mandatory
FPR_ANO_EXT.1	User Consent for Transmission of Personally Identifiable Information	Mandatory
FPT_API_EXT.1	Use of Supported Services and APIs	Mandatory
FPT_AEX_EXT.1	Anti-Exploitation Capabilities	Mandatory
FPT_TUD_EXT.1	Integrity for Installation and Update	Mandatory
FPT_TUD_EXT.2	Integrity for Installation and Update	Selection
FPT_LIB_EXT.1	Use of Third-Party Libraries	Mandatory
FPT_IDV_EXT.1	Software Identification and Versions	Mandatory
FTP_DIT_EXT.1	Protection of Data in Transit	Mandatory

5.3.1 Cryptographic Support (FCS)

FCS_CKM.1/AK Cryptographic Asymmetric Key Generation

FCS_CKM.1.1/AK The application shall [implement functionality] **to** generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm [

- **[ECC schemes]** using **[“NIST curves” P-384 and [P-256]** that meet the following: [**FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4**],

].

Application Note: This SFR was altered by TD0717.

FCS_CKM_EXT.1 Cryptographic Key Generation Services

FCS_CKM_EXT.1.1 The application shall [implement asymmetric key generation].

Application Note: This SFR was altered by TD0717.

FCS_CKM.2 Cryptographic Key Establishment

FCS_CKM.2.1 The application shall [implement functionality] to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- [Elliptic curve-based key establishment schemes] that meets the following: [NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”],
- [FFC Schemes using “safe-prime” groups] that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 7919]

].

FCS_COP.1/SKC Cryptographic Operation – Encryption/Decryption

FCS_COP.1.1/SKC The application shall perform [*encryption/decryption*] in accordance with a specified cryptographic algorithm [

- AES-CBC (as defined in NIST SP 800-38A) mode,
- AES-GCM (as defined in NIST SP 800-38D) mode,

] and cryptographic key sizes [128-bit, 256-bit].

Application note: This SFR was altered by TD0717.

FCS_COP.1/Hash Cryptographic Operation – Hashing

FCS_COP.1.1/Hash The application shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm [

- SHA-256,
- SHA-384,
- SHA-512

] and **message digest** sizes [

- 256,
- 384,
- 512

] **bits** that meet the following: [FIPS Pub 180-4].

FCS_COP.1/Sig Cryptographic Operation – Signing

FCS_COP.1.1/Sig The **application** shall perform [*cryptographic signature services (generation and verification)*] in accordance with a specified cryptographic algorithm [

- **RSA schemes** using cryptographic key sizes of [2048-bit or greater] that meet the following: [FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5],

].

Application note: This SFR was altered by TD0717.

FCS_COP.1/KeyedHash Cryptographic Operation – Keyed-Hash Message Authentication

FCS_COP.1.1/KeyedHash The **application** shall perform [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm [

- HMAC-SHA-256
- HMAC-SHA-384
- HMAC-SHA-512

] and [

- no other algorithms

] **with** key sizes [*256, 384, 512*] **and message digest sizes** [256, 384, 512] **and** [no other size] **bits** that meet the following: [*FIPS Pub 198-1, ‘The Keyed-Hash Message Authentication Code’ and FIPS Pub 180-4 ‘Secure Hash Standard’*].

Application note: This SFR was altered by TD0717.

FCS_RBG_EXT.1 Random Bit Generation Services

FCS_RBG_EXT.1.1 The application shall [invoke platform-provided DRBG functionality] for its cryptographic operations.

FCS_STO_EXT.1 Storage of Credentials

FCS_STO_EXT.1.1 The application shall [implement functionality to securely store [*file keys, safe keys, and password verifiers*] according to [FCS_COP.1/SKC]]

] to non-volatile memory.

FCS_TLS_EXT.1 TLS Protocol

FCS_TLS_EXT.1.1 The product shall implement [

- TLS as a server

].

FCS_TLSS_EXT.1 TLS Server Protocol

FCS_TLSS_EXT.1.1 The product shall implement TLS 1.2 (RFC 5246) and [no earlier TLS versions] as a server that supports the cipher suites [

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288

] and no other cipher suites, and also supports functionality for [

- none

].

Application Note: This SFR was altered by TD0779

FCS_TLSS_EXT.1.2 The product shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [TLS 1.1]

FCS_TLSS_EXT.1.3 The product shall perform key establishment for TLS using [

- Diffie-Hellman parameters with size [3072 bits] and no other sizes,
- ECDHE parameters using elliptic curves [secp256r1, secp384r1] and no other curves.

].

Application Note: This SFR was altered by TD0726.

5.3.2 User Data Protection (FDP)

FDP_DEC_EXT.1 Access to Platform Resources

FDP_DEC_EXT.1.1 The application shall restrict its access to [

- network connectivity

].

FDP_DEC_EXT.1.2 The application shall restrict its access to [

- [*the firewall, and event and system log repositories*]

].

FDP_NET_EXT.1 Network Communications

FDP_NET_EXT.1.1 The application shall restrict network communication to [

- user-initiated communication for *[the establishment of TLS sessions with the PAM components and the following functions:*
    - *CPM – authenticate to Password Vault Server, retrieve and update privileged passwords and password policies*

- *PSM – authenticate to Password Vault Server, retrieve privileged accounts, upload privilege session recordings*
- *PVWA – authenticate to Password Vault Server, TOE administration*
- *PSMP – authenticate to Password Vault Server, retrieve privileged accounts, upload privileged session recordings],*

] .

FDP_DAR_EXT.1 Encryption Of Sensitive Application Data

FDP_DAR_EXT.1.1 The application shall [

- leverage platform-provided functionality to encrypt sensitive data,
- protect sensitive data in accordance with FCS_STO_EXT.1,

] in non-volatile memory.

5.3.3 Security Management (FMT)

FMT_MEC_EXT.1 Supported Configuration Mechanism

FMT_MEC_EXT.1.1 The application shall [invoke the mechanisms recommended by the platform vendor for storing and setting configuration options].

FMT_CFG_EXT.1 Secure by Default Configuration

FMT_CFG_EXT.1.1 The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2 The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions [

- [*user management, configuration management, password management, start/stop service*]

].

5.3.4 Privacy (FPR)

FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1.1 The application shall [

- not transmit PII over a network,

].

5.3.5 Protection of the TSF (FPT)

FPT_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1 The application shall use only documented platform APIs.

FPT_AEX_EXT.1 Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1 The application shall not request to map memory at an explicit address except for [

- *0x0000000000000000*
- *0x000000007FFF0000*
- *0x000000007FFE0000*
- *0x000000007FFE1000*
- *0x000000007FFE3000*

].

FPT_AEX_EXT.1.2 The application shall [not allocate any memory region with both write and execute permissions].

FPT_AEX_EXT.1.3 The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4 The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5 The application shall be built with stack-based buffer overflow protection enabled.

FPT_TUD_EXT.1 Integrity for Installation and Update

FPT_TUD_EXT.1.1 The application shall [leverage the platform] to check for updates and patches to the application software.

FPT_TUD_EXT.1.2 The application shall [provide the ability] to view the current version of the application software.

FPT_TUD_EXT.1.3 The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4 Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5 The application is distributed [as an additional software package to the platform OS].

FPT_TUD_EXT.2 Integrity for Installation and Update

FPT_TUD_EXT.2.1 The application shall be distributed using the format of the platform-supported package manager.

FPT_TUD_EXT.2.2 The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

FPT_TUD_EXT.2.3 The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.

FPT_LIB_EXT.1 Use of Third Party Libraries

FPT_LIB_EXT.1.1 The application shall be packaged with only [*the libraries listed in Appendix B*].

FPT_IDV_EXT.1 Software Identification and Versions

FPT_IDV_EXT.1.1 The application shall be versioned with [[*version number*]].

5.3.6 Trusted Path/Channel (FTP)

FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1.1 The application shall [

- encrypt all transmitted [sensitive data] with [TLS as a server as defined in the Functional Package for TLS and also supports functionality for [none],

] between itself and another trusted IT product.

5.4 Assurance Requirements

20 The TOE security assurance requirements are summarized in Table 9.

Table 9: Assurance Requirements

Assurance Class	Components	Description
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.1	Security Objectives for the operational environment
	ASE_REQ.1	Stated Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM Coverage
	ALC_TSU_EXT.1	Timely Security Updates (as defined in PP_APP)
Tests	ATE_IND.1	Independent Testing – conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Analysis

6 TOE Summary Specification

6.1 Timely Security Updates

21 CyberArk endeavors to remediate critical and high severity publicly disclosed vulnerabilities in its TOEs, in accordance with their severity as implemented in the TOE, and subject to patches made available by their respective vendors (if applicable). The security updated can be provided as quickly as 4 weeks.

22 CyberArk will report a vulnerability to its customers when customers are required to take action to apply the remediation. Reporting of vulnerability-related issues may be via a security bulletin, release notes, knowledge base article, in-product notification or any other appropriate notification method. For the protection of CyberArk's customers, reporting of a vulnerability (including disclosure to any individual customer) will only be made once a remediation is made generally available by CyberArk, unless otherwise required by applicable law or regulation. In addition, the level of detail regarding a vulnerability in any reporting will be limited only to the minimum necessary.

23 If a security bulletin is issued, notification is sent via email to our technical subscribers (defined per customer upon request) and also published on the CyberArk website - Product Security | CyberArk, leading to a password-protected technical community - Login (site.com). First time users are asked to register prior to login.

6.2 SFR Fulfilment

24 Table 10 describes how the TOE fulfils the SFRs.

Table 10: SFR Fulfilment / TOE Summary Specification

SFR	Fulfilment
FCS_CKM.1/AK	Table 11 below lists all the key sizes used for the ECC asymmetric key generation scheme and its usage. Table 11 also lists the key establishment and key exchange schemes used by the TOE. The TOE uses ECDHE and DHE key establishment/exchange for TLS. The use of asymmetric encryption is needed for the TLS protocol used by the TOE. The key generation methods follow the requirements within FIPS PUB 186-4. The key establishment methods follow the requirements within NIST Special Publication 800-56A.
FCS_CKM_EXT.1	
FCS_CKM.2	
FCS_COP.1/SKC	AES128-CBC, AES256-CBC, AES128-GCM, AES256-GCM is used for the encryption/decryption of sensitive data stored in non-volatile memory.
FCS_COP.1/Hash	Table 12 lists all the key sizes used for SHA hashing and message digests within the TOE. SHA is used in TLS and SRP. The SHA256, SHA384, and SHA512 hash functions are used in HMAC for TLS message integrity and authentication. The TOE's implementation of SHA follows the requirements within FIPS Pub 180-4.

SFR	Fulfilment
FCS_COP.1/Sig	Table 11 lists all the key sizes used for signature generation and verification for TLS and the key sizes used to verify TOE file signatures. The TOE's implementation of signature generation and verification follow the requirements within FIPS PUB 186-4.
FCS_COP.1/KeyedHash	Table 12 lists all the key sizes used for SHA hashing and message digests within the TOE. SHA is used in TLS and SRP. The SHA256, SHA384, and SHA512 hash functions are used in HMAC for TLS message integrity and authentication. The TOE's implementation of SHA follows the requirements within FIPS Pub 180-4
FCS_RBG_EXT.1	The TOE implements the Approved SP 800-90 Approved AES256-CTR DRBG to generate random bits for key generation. When the TOE starts up, the DRBG is seeded with 256 bits of entropy from the Windows Entropy Pool by calling the OpenSSL **RAND_seed** function for the **CryptGenRandom** function and for Crypto API (CAPI). The platform system time and tick count noise sources are added to the Windows OS Entropy Pool after initialization. On an ongoing basis the TOE seeds the DRBG with 256 bits of entropy by calling the **RAND_seed** function for the **BCryptGenRandom** function and for the CNG (Crypto Next Generation) API. More information about the entropy process is described in the proprietary Entropy Rationale document.
FCS_STO_EXT.1	The TOE secures sensitive data stored in non-volatile memory using its algorithms for AES256-CBC encryption with a 256-bit key. Sensitive data includes the file key sent with a file from a PAM component, the Safe key used to encrypt the file key, and the verifier associated with a CyberArk password (for CyberArk authentication). • The privileged account file sent by a PAM client is encrypted by the PAM client. • The encrypted file is sent to the TOE and the file key is sent along securely in encrypted form over TLS. • The TOE decrypts the file key, then encrypts the file key with the Safe's unique AES 256-bit key using AES256-CBC encryption. • The Safe key is encrypted by the unique AES 256-bit Server key and stored within the Safe. A Safe key is generated automatically using the DRBG when a Safe is created. An administrator creates the initial password for a CyberArk (local) account. When the administrator creates the initial password, or a user changes it, the password is concatenated and manipulated using hash and exponential functions to derive a password verifier. The password verifier is stored in the MySQL DB. In the MySQL DB, the column containing the verifier is encrypted with the Server key using AES256-CBC encryption. Any time a local user authenticates, the password verifier is derived and authenticated against the value stored in the DB.

SFR	Fulfilment
	The Server key is unique to the TOE and is stored in volatile memory. The Server key is used to encrypt the Safe keys and the sensitive data stored within the DB. A Safe key is used to encrypt one or more files within a Safe. The Administrator user, and the PAM component users listed below, authenticate to the TOE using CyberArk authentication: • CPM – PasswordManager • PVWA – PVWAAppUser, PVWAGWUser • PSM – PSMAPPUSer, PSMGWUser • PSMP – PSMPAppUser, PSMPGWUser
FCS_TLS_EXT.1 FCS_TLSS_EXT.1	The TOE is a server to the OE PAM component clients. The TOE uses the https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/details?product=14798CyberArk Cryptographic Module v2.2.1 Module with the CyberArk libraries for the cryptographic services required to support TLS communications with the PAM component clients. The TOE uses X.509v3 certificates for TLS communications. The certificates are presented by the by the TOE during the TLS handshake is established. The vault certificates are authenticated by the connecting client, i.e. the Windows server PAM components, and the Linux server PAM components. The certificates can include (per generation) a CRL distribution point (CDP) to enable the clients to use a certificate revocation list (CRL) mechanisms to verify the certificate. The TOE supports: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 Six TLS suites are suggested by the components during the TLS handshake. These are: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128-GCM-SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 From these, the Vault server does not support ECDSA certificates. From the remaining four suites, the vault server will always select the strongest one available - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384.

SFR	Fulfilment
	Therefore, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 is the only ciphersuite used. The TOE does not accept any connection requests using SSL or a TLS version other than TLSv1.2. The TOE checks that the presented identifier matches the reference identifier, either the IP or DNS name, and only establishes a trusted channel if the identifier is a match and if the client’s certificate is validated. The TOE supports certificate pinning. Key agreement parameters are provided in Table 11: Cryptographic Algorithms.
FDP_DEC_EXT.1	The TOE limits its access to only network connectivity when accessing the platform’s hardware resources. The TOE requires network access to the CA server, the Windows server PAM components, and the RHEL server PAM components. The TOE limits access to only network connectivity between the PAM component clients and the TOE over TLS on port 443. The TOE also uses port 80 for HTTP connections to the CA server for certification revocation checks. The TOE limits access to the platform’s firewall services and audit mechanism. The TOE hardening process closes all ports and removes services not required by the TOE. The TOE accesses the platform’s firewall to take control over the firewall services and change the firewall information flow control rules. The TOE also accesses the platform’s audit mechanism to write event and system logs.
FDP_NET_EXT.1	
FDP_DAR_EXT.1	With the exception of cryptographic key destruction for keys stored in volatile memory, the TOE does not depend on platform-provided cryptographic functionality to provide its cryptographic services. The cryptographic functionality is included with the CyberArk Crypto Library, which provides all cryptographic services including encryption/decryption of data stored in Safes and in the MySQL DB. The TOE protects sensitive data by using AES256-CBC to encrypt the data before storing it in non-volatile memory and restricting access to the data. Sensitive data includes the file key used to encrypt a file sent by a PAM client, the Safe key used to encrypt the file key, and the password verifier used for SRP authentication to the TOE. The file key is encrypted by the Safe key of the Safe where it is stored. Both the client file and its encrypted file key are stored within the Safe. All sensitive data stored within a Safe is protected by that Safe’s key. The Safes are stored in non-volatile memory at c:\Private\Safes. The Safe key is encrypted with the 256-bit Server key using AES256-CBC encryption. The Server key is stored in volatile memory. The Administrator user and PAM components use SRP authentication. PAM client password verifiers are encrypted with the Server key using AES256-CBC encryption and stored in the MySQL DB. The sensitive data within a Safe is protected by the combination of the Vault Access Control Policy,

SFR	Fulfilment
	which is configured by the installation process, and the Safe Access Control Policy. Access to the Vault and Safes is enforced by user account authorizations and permissions. The Vault Access Control Policy controls user access to the Vault. The Vault Access Control Policy only allows access to the Vault for those users that are defined in the Vault.ini file. The Safe Access Control Policy controls Safe member permissions to view or create Safes and their permissions on the files within the Safes. An operator attempting to access the Vault or Safes with the incorrect authorizations and permissions is denied access. PSM and PSMP recordings may contain sensitive information if the user chooses to connect to a remote target which may contain sensitive information, therefore, we recommend the user to enable BitLocker.
FMT_MEC_EXT.1	The TOE uses OS functionality for storing and setting configuration options. The storage location of configuration files is maintained in the Windows Registry. The Server Windows Registry entries are located in the following file: HKLM\Software\CyberArk\PrivateArk\Server\. The TOE contains local configuration files that are created during installation, but the information is read-only and never written to by the TOE. The Administrator user or users in the Administrators group have Full control, Modify, Read & Execute, Read, and Write permissions for the configuration files. The configuration files are located in the C:\Program Files (x86)\PrivateArk\Server\conf folder. The DBParm.ini configuration file contains the general parameters for the Vault database. This file contains parameters for cryptographic algorithms, key locations, certificate settings, groups and users, and the TOE's listening port. The Passparm.ini file contains the password complexity settings.
FMT_CFG_EXT.1	Physical access is required for installation of the TOE. The TOE provides only enough functionality to enter credentials for the Administrator and Master users during installation. There are no default credentials for these users and no other default credentials stored on the TOE. Only an authorized administrator can install the TOE and set the credentials. During installation, the TOE is configured by default to protect the application's files from unauthorized access. The files are set with permissions that do not allow the Users group to modify them.
FMT_SMF.1	The TOE provides the following management functions: user management, configuration management, password management, start/stop service. Any other management operations must be performed by an authorized administrator using PVWA in the environment.
FPR_ANO_EXT.1	The TOE does not transmit PII. Usernames were considered and determined to not be PII as this information is owned and generated by the company that implements the TOE. This means that a Security

SFR	Fulfilment
	Policy must be enforced by the company that implements the TOE to prevent users from choosing their own personal username that could link to their personal identity.
FPT_API_EXT.1	The TOE uses only the standard platform APIs. Refer to Appendix A for a list of all APIs used by the TOE.
FPT_AEX_EXT.1	The TOE provides anti-exploitation protections. By default, ASLR protection is enabled on the Windows 2019 server. The TOE is compiled using the /NXCOMPAT flag to enable Data Execution Protection (DEP) and the /GS flag to enable stack-based buffer overflow protection. The TOE does not write user-modifiable files to directories that contain executable files. • Executable files are stored in ...\PrivateArk\Server\. • User-modifiable files are written to ...\PrivateArk\Server\Conf and ...\PrivateArk\Server\Logs. The TOE hardening is part of the installation and results in disablement of many operating system services. The hardening process also strips the permissions from existing and built-in Windows users (except the user that runs the installation). For more information about the hardening process, refer to the CyberArk Installation Guide and the script used to perform the hardening.
FPT_TUD_EXT.1/2 FPT_IDV_EXT.1	The TOE is delivered through CyberArk's online customer portal, which uses AWS Marketplace. The TOE installation and configuration files are all packaged into a zip file that is digitally signed by CyberArk. To verify the digital signature of a TOE package, users must do the following: 1. Download the TOE installation package from CyberArk. 2. Download and install the Java Development Kit (JDK) from Oracle. 3. Download and install the JCE Unlimited Strength Jurisdiction Policy Files. 4. Run the following command: JDK_Home%\jarsigner.exe -verify -verbose -certs .zip. More information about the jarsigner's options can be found at https://docs.oracle.com/javase/7/docs/technotes/tools/windows/jarsigner.html#CCHFIDAB. Individual TOE files are signed using the Windows OS package manager MS21 Sign tool. To verify the integrity of the TOE installation file, do the following: 1. Extract the files from the archive file. 2. Navigate to the setup.exe file. 3. Right-click the file, then click **Properties** > **Digital Signatures**.

SFR	Fulfilment
	4. Select the **CyberArk Software Ltd.** signer. Click **Details**, and then verify the signature details. The authorized signing source is CyberArk. The TOE relies on the platform's package manager to make changes to the binary code. Installation of the updates is performed by an administrator while using the executable file (.exe) extracted from the archive file (.zip). You can remove the TOE software from the platform using the platform's Programs and Features manager. Uninstallation of the TOE removes all traces of the application except for configuration settings, output files, and audit/log events. You can obtain the TOE version number by navigating to C:\CyberArk\Server_rls. Versioning naming convention: **AA.B.C.DD** (e.g: 14.0.0.32) - **AA** – Major Version Number – 14 - **B** – Minor Version Number – 0 - **C** – Patch Number – 0 - **DD** – Build Number - 32
FPT_LIB_EXT.1	The TOE is packaged with third-party libraries required for its functionality. For a full list, refer to Appendix B.
FTP_DIT_EXT.1	The TOE protects data in transit by providing trusted paths and channels using the cryptographic functions within the TOE's CyberArk PAM Cryptographic libraries. Communications between the TOE and Windows server's CPM, PSM, PVWA PAM components and between the TOE and RHEL server's PSMP PAM components are protected by TLS. The TOE acts as TLS server to the CPM, PSM, PVWA Windows components and to the PSMP PAM RHEL component. There is a single channel between the components and the TOE using TCP port 443.

Table 11: Cryptographic Algorithms

Operation	Usage	Algorithm	Key Size
Encryption/Decryption	Secure Storage	AES-CBC	256
	TLS	AES-GCM	128, 256
Key Generation	Safe	AES CTR-DRBG	256

Operation	Usage	Algorithm	Key Size
Signature Generation Signature Verification	TLS	RSA	2048, 3072, 4096
Key Exchange /Establishment	TLS	ECDHE, DHE	256, 384 3072
Message Digest	TLS	SHA-256, SHA-384, SHA-512	256, 384, 512
Message Authentication	TLS	HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	256, 384, 512
Random Number Generation	TOE DRBG	CTR DRBG (AES)	N/A

Table 12: HMAC

Hash Function	Block Size	Key Length	Output Digest
SHA256	512	256	256
SHA384	1024	384	384
SHA512	1024	512	512

7 Rationale

7.1 Conformance Claim Rationale

25 The following rationale is presented with regard to the PP conformance claims:

a) **TOE type.** As identified in section 1.2.1, the TOE is an application, consistent with the PP.

b) **Security problem definition.** As shown in section 3, the threats, OSPs and assumptions are reproduced in this ST.

c) **Security objectives.** As shown in section 4, the security objectives are reproduced in this ST.

d) **Security requirements.** As shown in section 5, the security requirements are reproduced from the PP. No additional requirements have been specified.

7.2 Security Objectives Rationale

26 All security objectives are drawn directly from the claimed PP.

Table 13: Security Objectives Rationale

Threat, Assumption, or OSP	Security Objectives	Rationale
T.NETWORK_ATTACK	O.PROTECTED_COMMS, O.INTEGRITY, O.MANAGEMENT	The threat T.NETWORK_ATTACK is countered by O.PROTECTED_COMMS because this provides for integrity of transmitted data. The threat T.NETWORK_ATTACK is countered by O.INTEGRITY because this provides for integrity of software that is installed onto the system from the network. The threat T.NETWORK_ATTACK is countered by O.MANAGEMENT because this provides for the ability to configure the application to defend against network attack.
T.NETWORK_EAVESDROP	O.PROTECTED_COMMS, O.QUALITY, O.MANAGEMENT	The threat T.NETWORK_EAVESDROP is countered by O.PROTECTED_COMMS because this provides for confidentiality of transmitted data. The objective O.QUALITY ensures use of mechanisms that provide protection against network-based attack. The threat T.NETWORK_EAVESDROP is

Threat, Assumption, or OSP	Security Objectives	Rationale
		countered by O.MANAGEMENT because this provides for the ability to configure the application to protect the confidentiality of its transmitted data.
T.LOCAL_ATTACK	O.QUALITY	The objective O.QUALITY protects against the use of mechanisms that weaken the TOE with regard to attack by other software on the platform.
T.PHYSICAL_ACCESS	O.PROTECTED_STORAGE	The objective O.PROTECTED_STORAGE protects against unauthorized attempts to access physical storage used by the TOE.
A.PLATFORM	OE.PLATFORM	The operational environment objective OE.PLATFORM is realized through A.PLATFORM.
A.PROPER_USER	OE.PROPER_USER	The operational environment objective OE.PROPER_USER is realized through A.PROPER_USER.
A.PROPER_ADMIN	OE.PROPER_ADMIN	The operational environment objective OE.PROPER_ADMIN is realized through A.PROPER_ADMIN.

7.3 Security Requirements Rationale

27 All security requirements are drawn directly from the claimed PP.

8 Appendix A

Platform API for dbmain.exe version 14.0.0.40

Contents of this file

1) Platform modules used

2) Platform API used per module

*** 1) Platform modules used ***

ADVAPI32.DLL

API-MS-WIN-CRT-CONIO-L1-1-0.DLL

API-MS-WIN-CRT-CONVERT-L1-1-0.DLL

API-MS-WIN-CRT-ENVIRONMENT-L1-1-0.DLL

API-MS-WIN-CRT-FILESYSTEM-L1-1-0.DLL

API-MS-WIN-CRT-HEAP-L1-1-0.DLL

API-MS-WIN-CRT-LOCALE-L1-1-0.DLL

API-MS-WIN-CRT-MATH-L1-1-0.DLL

API-MS-WIN-CRT-RUNTIME-L1-1-0.DLL

API-MS-WIN-CRT-STDIO-L1-1-0.DLL

API-MS-WIN-CRT-STRING-L1-1-0.DLL

API-MS-WIN-CRT-TIME-L1-1-0.DLL

API-MS-WIN-CRT-UTILITY-L1-1-0.DLL

BCRYPT.DLL

CRYPT32.DLL

DNSAPI.DLL

KERNEL32.DLL

MSCOREE.DLL

MSVCP140.DLL

NCRYPT.DLL

NTDSAPI.DLL

OLE32.DLL

OLEAUT32.DLL

RPCRT4.DLL

SECUR32.DLL

SHLWAPI.DLL

USER32.DLL

VCRUNTIME140.DLL

VCRUNTIME140_1.DLL

VERSION.DLL

WEBSERVICES.DLL

WS2_32.DLL

*** 2) Platform API used per module ***

ADVAPI32.DLL

CloseServiceHandle

ControlService

OpenSCManagerA

OpenServiceA

QueryServiceStatus

RegisterServiceCtrlHandlerA

SetServiceStatus

StartServiceCtrlDispatcherA

StartServiceA

AddAccessAllowedAce

AddAccessDeniedAce

CreateWellKnownSid

InitializeAcl

InitializeSecurityDescriptor

SetSecurityDescriptorDacl

RegCloseKey

RegOpenKeyA

RegOpenKeyExA

RegQueryValueExA

GetUserNameA

OpenProcessToken

OpenThreadToken

GetTokenInformation

LookupAccountSidA

GetSidSubAuthority

GetSidSubAuthorityCount

DeregisterEventSource

RegisterEventSourceW

ReportEventW

RegisterEventSourceA

ReportEventA

ChangeServiceConfigA

QueryServiceConfigA

RegEnumKeyExA

GetLengthSid

ConvertStringSidToSidA

ConvertStringSidToSidA

API-MS-WIN-CRT-CONIO-L1-1-0.DLL

_getch

API-MS-WIN-CRT-CONVERT-L1-1-0.DLL

atoi

_atoi64

atol

strtol

strtoul

_i64toa

_itoa

_i64toa_s

atof

_ultoa

strtod

_ltoa

wcstombs

_strtod_l

_atoi64

atoi

strtoul

API-MS-WIN-CRT-ENVIRONMENT-L1-1-0.DLL

getenv

getenv

API-MS-WIN-CRT-FILESYSTEM-L1-1-0.DLL

remove

rename

_stat64i32

rename

API-MS-WIN-CRT-HEAP-L1-1-0.DLL

free

malloc

calloc

_get_heap_handle

realloc

_callnewh

_aligned_free

_aligned_malloc

free

free

free

malloc

_callnewh

API-MS-WIN-CRT-LOCALE-L1-1-0.DLL

setlocale

localeconv

_configthreadlocale

_create_locale

_free_locale

_configthreadlocale

API-MS-WIN-CRT-MATH-L1-1-0.DLL

ceilf

log

_fdopen

__setusermatherr

fabs

fmod

pow

ceil

floor

asin

atan

atan2

cos

sin

sqrt

tan

ceilf

log

__setusermatherr

fabs

fmod

pow

asin

atan

atan2

cos

sin

sqrt

tan

API-MS-WIN-CRT-RUNTIME-L1-1-0.DLL

signal

_invalid_parameter_noinfo_noreturn

_errno

raise

_invalid_parameter_noinfo

perror

exit

_beginthreadex

strerror

system

_exit

abort

_seh_filter_exe

_set_app_type

_configure_narrow_argv

_initialize_narrow_environment

_get_initial_narrow_environment

_initterm

_initterm_e

__p___argc

__p___argv

_cexit

_c_exit

_register_thread_local_exe_atexit_callback

_initialize_onexit_table

_register_onexit_function

_crt_atexit

terminate

_getpid

_wassert

raise

exit

_exit

_seh_filter_exe

_set_app_type

_configure_narrow_argv

_initialize_narrow_environment

_get_initial_narrow_environment

_initterm

_initterm_e

__p___argc

__p___argv

_register_thread_local_exe_atexit_callback

_initialize_onexit_table

_register_onexit_function

_crt_atexit

API-MS-WIN-CRT-STDIO-L1-1-0.DLL

__acrt_iob_func

__stdio_common_vfprintf

__stdio_common_vsprintf

__stdio_common_vsscanf

fclose

fgetpos

fopen

fsetpos

_get_osfhandle

_filelengthi64

feof

fflush

fgets

fputs

fseek

ftell

__stdio_common_vsnprintf_s

fwrite

setvbuf

fread

ferror

__stdio_common_vsprintf_s

_get_stream_buffer_pointers

fgetc

fputc

_fseeki64

ungetc

putc

_wfopen

_fileno

_setmode

_close

_lseek

_read

_write

__stdio_common_vswprintf

_set_fmode

__p__commode

_wsopen_dispatch

_filelengthi64

__stdio_common_vsprintf

__stdio_common_vswprintf

_set_fmode

__p__commode

API-MS-WIN-CRT-STRING-L1-1-0.DLL

_strlwr

isdigit

isxdigit

tolower

strcspn

strncat

strncmp

strncpy

strtok_s

_stricmp

strnlen

strspn

strtok

strcpy_s

strcat_s

_strdup

toupper

_strupr

_strnicmp

isalpha

strcmp

isspace

isalnum

iscntrl

_wcsnicmp

isupper

strlen

strcpy

wcslen

strcat

_wcsupr

strtok_s

strcmp

strlen

strcpy

strcat

API-MS-WIN-CRT-TIME-L1-1-0.DLL

_mktime64

_ftime64

_gmtime64

_localtime64

_time64

_difftime64

_time32

__timezone

clock

strftime

__daylight

_localtime32

__dstbias

_gmtime64_s

__tzname

_tzset

_time64

API-MS-WIN-CRT-UTILITY-L1-1-0.DLL

qsort

bsearch

BCRYPT.DLL

BCryptGenRandom

BCryptGenRandom

CRYPT32.DLL

CertCreateCertificateContext

CertFreeCertificateContext

CertFreeCertificateChainEngine

CertGetCertificateChain

CertFreeCertificateChain

CertOpenStore

CertCloseStore

CertEnumCertificatesInStore

CertGetCertificateContextProperty

CryptProtectData

CryptUnprotectData

CryptProtectData

CryptUnprotectData

DNSAPI.DLL

DnsFlushResolverCacheEntry_A

KERNEL32.DLL

SetProcessShutdownParameters

FreeLibrary

GetProcAddress

LoadLibraryExA

SetConsoleCtrlHandler

GetLastError

SetLastError

Sleep

CreateFileA

GetFileAttributesA

SetFileAttributesA

WriteFile

CloseHandle

SetCurrentDirectoryA

GetCurrentDirectoryA

CreateDirectoryA

DeleteFileA

FindClose

FindFirstFileA

FindNextFileA

GetDiskFreeSpaceA

GetDriveTypeA

GetFileSizeEx

LockFile

ReadFile

RemoveDirectoryA

SetEndOfFile

SetFilePointerEx

SetFileTime

UnlockFile

QueryPerformanceCounter

GetCurrentProcessId

GetCurrentThreadId

GlobalMemoryStatusEx

GetSystemInfo

GetWindowsDirectoryA

GetModuleFileNameA

GetModuleHandleA

GetLogicalDriveStringsA

GetTempPathA

CopyFileA

MoveFileA

MoveFileExA

CompareFileTime

QueryPerformanceFrequency

GetSystemTime

SystemTimeToFileTime

MultiByteToWideChar

WideCharToMultiByte

LocalAlloc

LocalFree

GetCurrentProcess

GetCurrentThread

ConnectNamedPipe

DisconnectNamedPipe

SetNamedPipeHandleState

CreateNamedPipeA

SetEvent

CreateEventA

OpenEventA

MapViewOfFile

UnmapViewOfFile

CreateFileMappingA

OpenFileMappingA

SetThreadPriority

CreateMutexA

RtlCaptureContext

GetEnvironmentVariableA

SuspendThread

ResumeThread

GetThreadContext

GetVersionExA

ReadProcessMemory

GetProcessTimes

FileTimeToSystemTime

GetStdHandle

DuplicateHandle

InitializeCriticalSection

EnterCriticalSection

LeaveCriticalSection

TryEnterCriticalSection

DeleteCriticalSection

ResetEvent

ReleaseSemaphore

WaitForSingleObject

TerminateProcess

GetExitCodeProcess

TerminateThread

GetExitCodeThread

CreateProcessA

WaitForMultipleObjects

CreateSemaphoreA

GetEnvironmentStrings

FreeEnvironmentStringsA

HeapAlloc

HeapFree

GetProcessHeap

GetVersion

PostQueuedCompletionStatus

TlsAlloc

FormatMessageA

FormatMessageW

DeviceIoControl

LoadLibraryA

GetOverlappedResult

CreateIoCompletionPort

GetQueuedCompletionStatus

TlsGetValue

TlsSetValue

CreateFileW

GetFileAttributesW

SetFileAttributesW

GetFileType

GetModuleHandleW

RtlVirtualUnwind

GetSystemTimeAsFileTime

GetTickCount

LoadLibraryW

GlobalMemoryStatus

FindFirstFileW

FindNextFileW

GetFileSize

FlushConsoleInputBuffer

SetHandleInformation

CreatePipe

RtlLookupFunctionEntry

UnhandledExceptionFilter

SetUnhandledExceptionFilter

IsProcessorFeaturePresent

InitializeCriticalSectionAndSpinCount

WaitForSingleObjectEx

CreateEventW

IsDebuggerPresent

CreateDirectoryW

DeleteFileW

GetDiskFreeSpaceW

RemoveDirectoryW

GetWindowsDirectoryW

lstrcmpW

MoveFileW

MoveFileExW

GetACP

GetThreadLocale

GetLocaleInfoA

GetTimeZoneInformation

GetGeoInfoW

GetUserGeoID

GetLocaleInfoW

GetNumberFormatW

GetCurrencyFormatW

SystemTimeToTzSpecificLocalTime

GetDateFormatW

GetTimeFormatW

GetCurrentDirectoryW

GetFullPathNameW

GetFullPathNameA

SetFilePointer

IsValidCodePage

IsDBCSLeadByteEx

RaiseException

InitializeCriticalSectionEx

VirtualProtect

VirtualQuery

OutputDebugStringW

Sleep

CopyFileA

CreateDirectoryA

CloseHandle

SetEndOfFile

FindClose

FindFirstFileA

FindNextFileA

GetCurrentDirectoryA

SetCurrentDirectoryA

CompareFileTime

GetSystemTime

SystemTimeToFileTime

WideCharToMultiByte

CreateNamedPipeA

DisconnectNamedPipe

ReadFile

WriteFile

InitializeCriticalSection

CreateEventA

CreateSemaphoreA

DeleteCriticalSection

EnterCriticalSection

GetCurrentProcessId

GetCurrentThreadId

GetExitCodeThread

LeaveCriticalSection

ReleaseSemaphore

ResetEvent

SetEvent

TerminateThread

TryEnterCriticalSection

FreeEnvironmentStringsA

GetEnvironmentStrings

GetEnvironmentVariableA

LeaveCriticalSection

FreeLibrary

GetProcAddress

LoadLibraryA

GetLastError

GetTempPathA

LocalFree

InitializeCriticalSectionEx

MSCOREE.DLL

_CorExeMain

MSVCP140.DLL

_Strcoll

_Strxfrm

_Xtime_get_ticks

_Mtx_init_in_situ

_Mtx_destroy_in_situ

_Mtx_lock

_Mtx_unlock

_Query_perf_counter

_Query_perf_frequency

_Strcoll

_Strxfrm

_Xtime_get_ticks

_Mtx_init_in_situ

_Mtx_destroy_in_situ

_Mtx_lock

_Mtx_unlock

_Query_perf_counter

_Query_perf_frequency

_Xlength_error

uncaught_exception

_Xbad_alloc

_Xout_of_range

_Xregex_error

_Throw_C_error

_Xbad_function_call

_Xinvalid_argument

_Fiopen

setw

_Syserror_map

_Xbad_alloc

_Xregex_error

_Throw_C_error

_Xbad_function_call

_Xinvalid_argument

_Fiopen

setw

_Syserror_map

_Getcvt

_Locinfo

~_Locinfo

_Getfalse

_Gettrue

_Getcoll

_Getlconv

_Lockit

~_Lockit

operator=

~basic_ios<charCOMMABREAKstruct_std::char_traits<char>_>

setstate

widen

basic_ios<charCOMMABREAKstruct_std::char_traits<char>_>

clear

imbue

basic_iostream<charCOMMABREAKstruct_std::char_traits<char>_>

~basic_iostream<charCOMMABREAKstruct_std::char_traits<char>_>

basic_istream<charCOMMABREAKstruct_std::char_traits<char>_>

~basic_istream<charCOMMABREAKstruct_std::char_traits<char>_>

_Ipfx

operator>>

operator>>

get

operator>>

seekg

tellg

read

basic_ostream<charCOMMABREAKstruct_std::char_traits<char>_>

~basic_ostream<charCOMMABREAKstruct_std::char_traits<char>_>

_Osfx

operator<<

operator<<

operator<<

put

flush

write

`vbase_destructor'

operator<<

operator<<

operator<<

operator<<

operator<<

basic_streambuf<charCOMMABREAKstruct_std::char_traits<char>_>

~basic_streambuf<charCOMMABREAKstruct_std::char_traits<char>_>

sbumpc

sgetc

sputc

sputn

_Pninc

_Lock

_Unlock

imbue

setbuf

showmanyc

sync

uflow

xsgetn

xsputn

getloc

snextc

_Init

pbase

eback

gptr

pptr

egptr

epptr

_Lock

_Unlock

imbue

setbuf

showmanyc

sync

uflow

xsgetn

xsputn

always_noconv

in

out

unshift

_Getcat

~codecvt<unsigned_shortCOMMABREAKcharCOMMABREAKstruct__Mbstatet>

codecvt<unsigned_shortCOMMABREAKcharCOMMABREAKstruct__Mbstatet>

out

toupper

_Getcat

tolower

tolower

widen

narrow

exceptions

getloc

classic

_Init

_Getgloballocale

classic

_Init

_Getgloballocale

_New_Locimp

_Addfac

facet

~facet

_Decref

_Incref

_Decref

_Incref

operator_unsigned___int64

NCRYPT.DLL

NCryptOpenStorageProvider

NCryptOpenKey

NCryptGetProperty

NCryptExportKey

NCryptFreeObject

NCryptOpenStorageProvider

NCryptOpenKey

NCryptGetProperty

NCryptExportKey

NCryptFreeObject

NTDSAPI.DLL

DsFreePasswordCredentials

DsMakePasswordCredentialsW

OLE32.DLL

IIDFromString

CoUninitialize

CoInitializeEx

CoCreateInstance

OLEAUT32.DLL

SysAllocStringLen

SysFreeString

VariantInit

VariantClear

VariantChangeType

VariantClear

RPCRT4.DLL

RpcStringFreeA

UuidCreate

UuidToStringA

RpcBindingSetOption

RpcBindingFromStringBindingW

RpcStringBindingComposeW

RpcBindingSetAuthInfoExW

RpcStringFreeW

RpcBindingFree

I_RpcBindingInqSecurityContext

NdrClientCall2

SECUR32.DLL

FreeContextBuffer

QueryContextAttributesW

SHLWAPI.DLL

PathFileExistsA

PathFindExtensionA

PathFindFileNameA

PathIsDirectoryA

PathMatchSpecA

PathRemoveFileSpecA

PathStripToRootA

PathFileExistsW

PathIsDirectoryW

PathRemoveFileSpecW

UrlUnescapeW

StrCmpW

StrCmpIW

PathIsDirectoryA

PathFileExistsA

PathFindExtensionA

PathFindFileNameA

PathMatchSpecA

PathRemoveFileSpecA

PathStripToRootA

USER32.DLL

CharLowerA

CharUpperA

GetProcessWindowStation

GetUserObjectInformationW

MessageBoxW

GetDesktopWindow

VCRUNTIME140.DLL

memset

longjmp

__std_exception_copy

__std_exception_destroy

_CxxThrowException

memcpy

memmove

strchr

strstr

_purecall

__C_specific_handler

__std_type_info_name

memchr

memcmp

strrchr

__std_type_info_compare

__std_type_info_hash

__RTDynamicCast

wcsstr

__intrinsic_setjmp

__current_exception

__current_exception_context

__RTtypeid

__FrameUnwindFilter

memset

longjmp

memcpy

strchr

strstr

_purecall

__C_specific_handler

__std_type_info_name

memchr

memcmp

strrchr

__std_type_info_compare

__std_type_info_hash

wcsstr

__intrinsic_setjmp

__RTtypeid

VCRUNTIME140_1.DLL

__CxxFrameHandler4

__CxxFrameHandler4

VERSION.DLL

GetFileVersionInfoSizeA

GetFileVersionInfoA

VerQueryValueA

GetFileVersionInfoSizeA

GetFileVersionInfoA

VerQueryValueA

WEBSERVICES.DLL

WsCreateError

WsGetErrorString

WsFreeError

WsCreateHeap

WsFreeHeap

WsOpenServiceProxy

WsCloseServiceProxy

WsFreeServiceProxy

WsCall

WsCreateServiceProxyFromTemplate

WsCreateError

WsGetErrorString

WsFreeError

WsCreateHeap

WsFreeHeap

WsOpenServiceProxy

WsCloseServiceProxy

WsFreeServiceProxy

WsCall

WsCreateServiceProxyFromTemplate

WS2_32.DLL

getaddrinfo

freeaddrinfo

inet_pton

inet_ntop

accept

bind

closesocket

connect

getpeername

getsockname

getsockopt

htonl

htons

ioctlsocket

inet_addr

inet_ntoa

listen

ntohl

ntohs

recv

recvfrom

select

send

sendto

setsockopt

shutdown

socket

gethostbyname

gethostname

WSAGetLastError

WSASetLastError

WSAStartup

WSACleanup

__WSAFDIsSet

__WSAFDIsSet

inet_addr

inet_ntop

9 Appendix B

c:\Program Files (x86)\PrivateArk\Server\libcrypto-1_1-x64.dll

c:\Program Files (x86)\PrivateArk\Server\libcurl.dll

c:\Program Files (x86)\PrivateArk\Server\libeay32.dll

c:\Program Files (x86)\PrivateArk\Server\libmysql.dll

c:\Program Files (x86)\PrivateArk\Server\libprotobuf-lite.dll

c:\Program Files (x86)\PrivateArk\Server\libprotobuf.dll

c:\Program Files (x86)\PrivateArk\Server\libsasl.dll

c:\Program Files (x86)\PrivateArk\Server\libssl-1_1-x64.dll

c:\Program Files (x86)\PrivateArk\Server\PARENEAgent.dll

c:\Program Files (x86)\PrivateArk\Server\PARNotificator.dll

c:\Program Files (x86)\PrivateArk\Server\PARVaultAgent.dll

c:\Program Files (x86)\PrivateArk\Server\RacControllerSDK.dll

c:\Program Files (x86)\PrivateArk\Server\ssleay32.dll

c:\Program Files (x86)\PrivateArk\Server\Xalan-C_1_12_x64.dll

c:\Program Files (x86)\PrivateArk\Server\XalanMessages_1_12_x64.dll

c:\Program Files (x86)\PrivateArk\Server\xerces-c_3_2_2_x64.dll

c:\Program Files (x86)\PrivateArk\Server\Database\Bin\libcrypto-1_1-x64.dll

c:\Program Files (x86)\PrivateArk\Server\Database\Bin\libcurl.dll

c:\Program Files (x86)\PrivateArk\Server\Database\Bin\libprotobuf-lite.dll

c:\Program Files (x86)\PrivateArk\Server\Database\Bin\libprotobuf.dll

c:\Program Files (x86)\PrivateArk\Server\Database\Bin\libsasl.dll

c:\Program Files (x86)\PrivateArk\Server\Database\Bin\libssl-1_1-x64.dll

c:\Program Files (x86)\PrivateArk\Server\Database\MySQL Utilities\msvcp120.dll

c:\Program Files (x86)\PrivateArk\Server\Database\MySQL Utilities\msvcr120.dll

c:\Program Files (x86)\PrivateArk\Server\Database\MySQL Utilities\python27.dll

c:\Program Files (x86)\PrivateArk\Server\Event Notification Engine\libeay32.dll

c:\Program Files (x86)\PrivateArk\Server\Event Notification Engine\ssleay32.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\CyberArk.AppServices.Jwt.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\CyberArk.AppServices.LogicContainer.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\CyberArk.Casos.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\CyberArk.Infra.Logger.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\CyberArk.Services.Exceptions.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\log4net.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PowerCollections.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDlls\Cyberark.DNA.Shared.Models.dll c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDlls\Cyberark.DNA.Shared.ModelsContract.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDlls\CyberArk.LogicContainer.Shared.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDlls\FluentNHibernate.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDlls\Iesi.Collections.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDlls\Microsoft.IdentityModel.Logging.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDlls\Microsoft.IdentityModel.Tokens.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDlls\MySql.Data.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDlls\Newtonsoft.Json.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDlls\NHibernate.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDlls\NHibernate.XmlSerializers.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDlls\PIMSuiteBL.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDlls\PIMSuiteData.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDlls\System.IdentityModel.Tokens.Jwt.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\BLDlls\WorkFlowManager.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\BouncyCastle.Crypto.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\Castle.Core.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\Castle.Windsor.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Data.Entities.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Data.Messaging.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Data.Messaging.Policies.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Infra.Base.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Infra.Common.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Infra.Engine.Contracts.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Infra.Engine.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Adapters.PIM.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Data.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Engine.Contracts.Adapters.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Engine.Contracts.App.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Engine.Contracts.Packages.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Engine.dll c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Packages.Accounts.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Packages.Base.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Packages.BulkOperations.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Packages.Contracts.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Packages.Data.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Packages.Policies.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\CyberArk.Server.Packages.Users.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\Dapper.StrongName.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\K4os.Compression.LZ4.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\K4os.Compression.LZ4.Streams.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\K4os.Hash.xxHash.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\MySql.Data.dll

c:\Program Files (x86)\PrivateArk\Server\LogicContainer\PlugIns\System.Buffers.dll